# Kritische beoordeling van het gebruik van de Belgische eID kaart

Bart De Decker[†], Vincent Naessens[‡], Jorn Lapon[‡], Pieter Verhaeghe[†]
† K.U.Leuven, Departement Computerwetenschappen
‡ Katholieke Hogeschool Sint-Lieven, Gent, vakgroep IT

Mei, 2008

Het onoordeelkundig gebruik van de huidige Belgische identiteitskaart houdt gevaren in voor de kaarthouder. Niet alleen kan zijn privacy geschonden worden, het kan ook aanleiding geven tot bedrog en kan verstrekkende gevolgen hebben voor de burger. In dit document proberen we een overzicht te geven van deze gevaren. We moeten hierbij opmerken dat niet alle gevaren kunnen afgeschermd worden door een aanpassing van de software.

Aangezien verschillende drukkingsgroepen in onze maatschappij er op aandringen dat de overheid het gebruik van de kaart promoot, willen we toch tot voorzichtigheid aansporen. Zolang de meeste problemen niet opgelost zijn, lijkt het ons niet aangewezen om de kaart op grote schaal te gaan gebruiken.

De problemen worden in dit rapport onderverdeeld volgens hun voornaamste oorzaak:

1. de eID kaart zelf,
2. de door Fedict geleverde software,
3. de computer (met bijbehorend besturingssysteem) waarop de kaart gebruikt wordt.

Uiteraard worden sommige problemen veroorzaakt door een combinatie van deze factoren.

De problemen zijn niet "hypothetisch"; voor verschillende scenario's die in dit rapport beschreven worden, zijn prototypes beschikbaar.

Verschillende scenario's zijn strafbaar volgens de Belgische en Europese regelgeving; helaas stopt het Internet niet bij de Belgische of Europese grenzen.

## 1 Problemen gerelateerd aan de eID kaart zelf

In deze sectie zullen we het niet hebben over de fysische problemen zoals het **loskomen van de chip**, waardoor de identiteitskaart onbruikbaar wordt. Dit kan echter wel verregaande gevolgen hebben voor de kaarthouder. Naarmate het gebruik van de kaart toeneemt zullen dergelijke defecten als gevolg hebben dat personen gedurende een behoorlijk lange tijd uitgesloten zullen worden van bepaalde diensten en bepaalde lokaties. Zolang de overheid niet kan garanderen dat een vervangkaart reeds de volgende dag beschikbaar is (zoals dit met kredietkaarten bijv. het geval is), zou het gebruik van de kaart eerder moeten ontmoedigd worden.

## 1.1 Rijksregisternummer en Big Brother

Het veelvuldig gebruik van de eID kaart leidt tot **Big Brother** toestanden. Aangezien de twee certificaten in de kaart het **rijksregisternummer** bevatten, kunnen alle transacties waarbij de kaart gebruikt wordt, gelinkt worden aan de kaarthouder en aan elkaar. Wettelijk gezien mag men dit nummer niet gebruiken, maar de oplossing die door vele bedrijven wordt aangewend is het *hashen* van dit nummer. Er zijn echter slechts een beperkt aantal hash-functies beschikbaar, zodat er nog steeds een uniek nummer geassocieerd wordt met elke persoon. Via dit nummer kunnen records uit verschillende gegevensbanken (van verschillende organisaties) met elkaar verbonden worden, wat aanleiding kan geven tot zeer uitgebreide gebruikersprofielen. Merk ook op dat de ontvanger van het certificaat uit het rijksregisternummer de geboortedatum en het geslacht van de houder kan afleiden.

Bij het ondertekenen van een document zal de ontvanger van de handtekening zowel de handtekening zelf als het certificaat moeten opslaan, om in geval van betwisting te kunnen bewijzen dat de handtekening authentiek is. Bijgevolg moet het rijksregisternummer in leesbare vorm opgeslagen worden.

## 1.2 Geen toegangscontrole

Een groot probleem van de kaart is dat er **geen toegangscontrole** voorzien is op de kaart zelf. In principe kan elke toepassing, zonder toestemming van de burger, de drie bestanden (digitale foto, identiteitsgegevens en adres) en de twee certificaten uitlezen. Fedict heeft dit probleem proberen op te lossen via een programma, de *privacy service*, die de kaartlezer vergrendelt en toepassingen verplicht gebruik te maken van de Fedict software. De Fedict software zal bij "sommige" uitleesoperaties de toelating aan de gebruiker vragen. Dit is echter niet waterdicht (cfr. sectie 2.1).

In bepaalde gevallen kan het stiekem uitlezen van de kaart tot gevaarlijke situaties leiden.

**Veilig chatten op het Internet**

Reeds enige tijd kunnen kinderen "veilig" chatten op het Internet. Hiertoe gebruiken ze hun identiteitskaart. De veilige chatsite[a] controleert de leeftijd van de gebruiker, en zal alleen kinderen toelaten. Stel dat zo'n kind op deze site aanlogt. In een ander venster van de browser speelt het een spelletje (een applet die van een website komt die beheerd wordt door een pedofiel). De applet kan de foto, persoonsgegevens en adresgegevens van de eID kaart uitlezen en doorsturen naar de site van de pedofiel. Hij beschikt dus binnen de kortste keren over een hele database met mogelijke toekomstige slachtoffers, van wie hij niet alleen een foto, maar ook naam, leeftijd en adresgegevens heeft.
Ook spyware[b] die op de computer aanwezig zou zijn, kan mogelijk ongemerkt deze gegevens uitlezen en doorspelen naar om het even welke site. Zelfs als software deze toegang zou onderscheppen, dan zullen de meeste kinderen de waarschuwing negeren en de toegang toestaan.

[a] Merk op dat zo'n chatsite nooit kan garanderen dat er alleen maar kinderen toegelaten worden op de site. De enige garantie die men heeft is dat alle aanwezigen beschikken over een identiteitskaart die toebehoort aan een kind. Een pedofiele ouder kan gemakkelijk een eID kaart van zijn/haar kind lenen en waarom zou een pedofiel niet de kaart kunnen lenen van een van zijn slachtoffers? Een "veilige chatsite" is in een bepaald opzicht onveiliger dan een gewone chatsite: bij deze laatste verwacht men tenminste dat er mensen met minder goede bedoelingen aanwezig zijn, terwijl men **ten onrechte** denkt dat de eerste veilig is.

[b] Computers die intensief door kinderen gebruikt worden, worden vrij snel besmet door allerlei spyware.

Aangezien de kaart geen toegangscontrole uitvoert, wordt het problematisch wanneer de burger zijn eID kaart op een andere (vreemde) computer moet gebruiken. Daar heeft men helemaal geen controle over welke software[1] er al dan niet draait.

**Toegang tot sauna of fitness-centrum**

Steeds meer fitness- en sauna-centra overwegen de eID kaart te gebruiken om klanten toegang te geven tot deze centra. Zodra de kaart in de kaartlezer wordt gestoken, kan in principe alle informatie uitgelezen worden. Veronderstel even dat op deze computer spyware draait (die per ongeluk of moedwillig geïnstalleerd is). De klantgegevens (waaronder het adres) kunnen in dit geval doorgestuurd worden naar een criminele organisatie. Deze laatste mag verwachten dat de klant enige uren in dit centrum zal verblijven zodat ze ruim de tijd heeft om de woning van deze klant te "bezoeken".

## 1.3 Single Sign-On

Voor authenticatie voorziet de kaart "single sign-on" (SSO), dit betekent dat men slechts eenmaal zijn PIN-code ingeeft, en daarna een onbeperkt aantal keren kan authenticeren. Alhoewel dit misschien "gebruiksvriendelijk" lijkt, houdt het enorme risico's in voor de kaarthouder.

**Een elektronische dienst**

Een klant logt in (met zijn eID kaart), op een site met behulp van een ondertekende applet (die in een browser uitgevoerd wordt) of via een toepassing die op de computer gedownload werd. Terwijl de gegevens geladen worden, kan de applet of toepassing heimelijk inloggen in `mijndossier`, `taxonweb`, `MyMinFin` en tal van andere diensten die toegankelijk zijn met de eID kaart, en de daar beschikbare gegevens (zoals loonfiches, belastingsformulieren, ...) over de klant opvragen (en zelfs wijzigen!). Het spreekt vanzelf dat dit een enorm risico inhoudt voor de burger. Merk ook op dat eenmaal de privacy van een individu geschonden is, bijv. omdat deze gegevens op het Internet geplaatst werden, deze privacy nooit meer hersteld kan worden.

In principe kan men in het configuratie-bestand aangeven dat 'single sign-on' niet toegelaten is. De gebruiker zal dan voor elke authencatie een PIN-code moeten ingeven. Helaas werkt dit niet. Bij nazicht in de broncode, blijkt dat deze optie onvolledig geïmplementeerd is! Bij het afzetten van SSO lukt authenticatie helemaal niet meer.

Mocht dit "afzetten van de SSO" toch voorzien zijn in de software, dan blijft dit flagrante misbruik toch mogelijk indien de applet of toepassing geen gebruik maakt van de software die door Fedict geleverd wordt, maar rechtstreeks de kaartlezer aanspreekt.

## 1.4 Geen transparantie in het gebruik van de kaart

In de vorige sectie werd reeds vermeld dat een toepassing een onbeperkt aantal authenticaties kan vragen aan de kaart, zonder dat de gebruiker hier iets van merkt.

Een belangrijk nadeel aan het gebruik van de eID kaart is dat men als gebruiker de software moet vertrouwen dat ze de correcte informatie verschaft over de operatie

[1] Zelfs met een actieve privacy service heeft men geen enkele garantie; de eigenaar van de computer kan immers vooraf reeds aan de software hebben gemeld dat een bepaald programma **altijd** de kaart mag uitlezen.

die uitgevoerd zal worden op deze kaart (zie ook sectie 2.2). De software kan de gebruiker misleiden (dit is niet zo moeilijk aangezien men rechtstreeks de driver van de kaartlezer kan aanspreken, zonder gebruik te maken van de software van Fedict).

Doordat dezelfde PIN-code gebruikt wordt voor authenticatie en het plaatsen van een handtekening, kan de gebruiker bedrogen worden. De toepassing kan de gebruiker vragen om zich te authenticeren, terwijl aan de kaart gevraagd wordt om iets te ondertekenen. Aangezien de handtekeningen wettelijk erkend worden, kan dit verregaande gevolgen hebben voor de betrokken burger.

# 2 Software geleverd door Fedict

Het is niet noodzakelijk om de software die door Fedict geleverd wordt te installeren en op te starten om gebruik te kunnen maken van de eID kaart. Tegenmaatregelen die dus uitsluitend gerealiseerd worden door Fedict software kunnen redelijk eenvoudig omzeild worden. Alleen wanneer de privacy service draait op de PC, kan verhinderd worden dat toepassingen rechtstreeks de kaartlezer aanspreken.

## 2.1 Toegangscontrole door de software

Aangezien de eID kaart geen toegangscontrole uitvoert, gebeurt deze in de door Fedict geleverde software, de **beid[2]-middleware**. Om te vermijden dat toepassingen andere software zouden gebruiken voor het aanspreken van de eID kaart, voorziet men ook nog een speciale toepassing, de **privacy service**, die als enige doel heeft de kaartlezer te vergrendelen en dus als doorgeefluik van/naar de eID kaart fungeert voor de beid-middleware.

De beid-software kent echter heel wat problemen:

- De beid-middleware beschouwt bepaalde programma's als 'betrouwbaar' (zoals browsers: Internet Explorer, Firefox, Netscape, ...), zodat voor deze programma's geen toelating gevraagd wordt. Nochtans kan je net met deze programma's de kaart misbruiken.

  Het volstaat dus de naam van een schadelijk programma te veranderen in een van de 'vertrouwde' programma's om de toegangscontrole van de beid-software te omzeilen (zoals in het YouTube filmpje werd geïllustreerd: `http://belsec.skynetblogs.be/post/5870586`).

- Indien beid-middleware wel een uitlees-operatie onderschept, zal zij via een pop-up venster de goedkeuring of afkeuring vragen aan de gebruiker. Het valt te betwijfelen[3] of gebruikers hierop gepast zullen reageren. De kans is reëel dat men gewoon de toestemming geeft omdat 'het anders niet werkt'.

- Men kan niet op een eenvoudige manier nagaan voor welke toepassingen de beid-middleware geen toestemming zal vragen aan de gebruiker bij een uitleesoperatie. Het is ook niet duidelijk hoe men een eerder gegeven toestemming terug kan intrekken.

Ook de privacy service heeft nadelen:

[2] **B**elgian **eID**-middleware

[3] Gebruikers moeten voor bepaalde diensten ook al "minder veilige" beslissingen nemen indien ze gebruik wensen te maken van bepaalde overheidsdiensten: het server-certificaat van `https://mijndossier.rrn.fgov.be/` kan niet geverifieerd worden, en de gebruiker is verplicht een "onveilig" certificaat te aanvaarden om deze site te kunnen bezoeken.

- De privacy service vergrendelt de kaartlezer, zodat ze niet meer voor andere doeleinden kan gebruikt worden, bijv. voor transacties met een bankkaart. Een aantal banken stelt dan ook tools ter beschikking om deze privacy service af te zetten (cfr. `http://www.kbc.be/welkom` ⇒ *"Problemen voorkomen met eID-software voor de elektronische identiteitskaart"*). Eenmaal dat de privacy service afgezet is, kan elke toepassing die niet gebruik maakt van de beid-software, de gegevens uitlezen en doorsturen via het Internet naar om het even welke site.

- Het is niet moeilijk om de privacy service af te zetten. Het kan zelfs stiekem gebeuren zonder dat de gebruiker hiervan weet heeft. Op de meeste computers heeft de gebruiker administratieve rechten, waardoor men onbeperkt configuratie-bestanden kan aanpassen, nieuwe programma's kan installeren, weglaten of zelfs wijzigen. Bijvoorbeeld spyware kan ervoor zorgen dat de privacy service bij de volgende opstart van de computer niet meer automatisch gestart wordt.

- Het is in principe niet onmogelijk dat ook andere software de privacy service als doorgeefluik gebruikt. In dat geval is er helemaal geen toegangscontrole meer.

## 2.2 Te weinig transparantie in het gebruik van de eID kaart

De beid-software brengt de gebruiker via pop-up vensters op de hoogte van een op handen zijnde operatie (uitlezen informatie, authenticatie of het plaatsen van een handtekening). De layout van de vensters is niet consequent:

- Het venster dat getoond wordt bij het uitlezen wordt alleen getoond als de toepassing niet vertrouwd wordt. In het venster worden de naam van de toepassing en de bestanden die uitgelezen zullen worden getoond.

- Bij authenticatie wordt alleen de eerste keer een PIN-code opgevraagd. De gebruiker blijft in het ongewisse welke toepassing de authenticatie opstart, en met welke site authenticatie zal gebeuren. Dit kan aanleiding geven tot misbruiken die eerder reeds vermeld werden: bijvoorbeeld de gebruiker denkt dat hij inlogt op site XYZ, maar in plaats daarvan logt de toepassing in op `TaxOnWeb`.

  Vanaf de tweede authenticatie wordt er geen venster meer getoond en blijft de authenticatie verborgen voor de gebruiker.

- Bij het plaatsen van een handtekening, vraagt het pop-up venster de PIN-code en wijst ze de gebruiker op het feit dat er een handtekening zal geplaatst worden. De gebruiker kan eventueel de operatie voortijdig afbreken.

  Het venster toont echter niet welk bestand zal getekend worden, noch de hash-waarde van het bestand. Dit betekent dat een totaal ander bestand ter ondertekening kan aangeboden worden dan de toepassing laat uitschijnen aan de gebruiker.

Merk ook op dat een toepassing de beid-software niet hoeft te gebruiken, en zelf gelijkaardige pop-ups kan tonen aan de gebruiker. In dit geval kan de gebruiker zelfs volledig misleid worden: het pop-up venster meldt dat een authenticatie gevraagd wordt terwijl aan de kaart gevraagd wordt om iets te ondertekenen. Dit misbruik is mogelijk omdat dezelfde PIN-code gebruikt wordt voor zowel authenticatie als het plaatsen van een handtekening (cfr. sectie 1.4).

### 2.3 Vragen over de kwaliteit van de software

In de vorige sectie werd reeds aangehaald dat bijvoorbeeld het afzetten van de single sign-on optie onvolledig geïmplementeerd werd.

Bij het inspecteren van de bron-code[4], kan men op heel wat plaatsen commentaar vinden zoals `/* FIXME ... */`, `/* correct? */`, `/* to be implemented */`. Dergelijke commentaar wijst er op dat de software onvoldoende is uitgetest en te vroeg beschikbaar werd gesteld.

De documentatie is waarschijnlijk niet helemaal up-to-date en niet in overeenstemming met de implementatie. Het is bijvoorbeeld niet duidelijk welke software component de toegangscontrole bij het uitlezen van de eID kaart uitvoert.

In de software worden C-functies gebruikt (zoals `strcpy`), die als onveilig beschouwd worden en mogelijk aanleiding kunnen geven tot bufferoverloop-aanvallen.

Tenslotte merken we op dat bepaalde overheidsdiensten (o.a. "Mijn dossier") nog steeds een webserver draaien, Microsoft IIS 5.0, die standaard meegeleverd is met Windows Server 2000. Men kan zich afvragen of deze webserver gekende zwakheden voldoende kan afschermen: worden de gegevens van de gebruikers voldoende beschermd en is de website bestand tegen defacement-aanvallen?

## 3 De computer en bijbehorende besturingssysteem

### 3.1 De kaartlezer

Op de meeste computers is slechts een primitieve kaartlezer aanwezig: d.w.z. een kaartlezer zonder venster en zonder pinpad[5]. Het is ook dit type kaartlezer dat door de overheid gratis aan kinderen werd ter beschikking gesteld.

Aangezien er geen venster aanwezig is, kan de gebruiker niet controleren wat er precies aan de kaart gevraagd wordt, en eventueel een operatie onderbreken (via een abort-toets).

Doordat er geen pinpad aanwezig is, moeten PIN-codes via het klavier van de computer in een pop-up venster worden ingebracht. Spyware en keyboard loggers kunnen toetsaanslagen onderscheppen. Hierdoor beschikken ze over de PIN-code en kunnen ze deze later misbruiken. Een toepassing zou dan zonder dat de gebruiker dit merkt, kunnen inloggen in tal van websites en de eID kaart bestanden laten ondertekenen!

**Verzekeringsagent**

Het is niet ondenkbaar dat een klant door een verzekeringsagent verleid wordt om een "goedkope" polis elektronisch te ondertekenen. Indien de klant zijn PIN-code intypt op de computer van deze makelaar, kan deze zonder dat de gebruiker dit merkt, inloggen op tal van sites, en informatie verzamelen over de klant. Het (onrechtmatig) afhalen en analyseren van persoonlijk informatie kan leiden tot een duurdere polis in de toekomst. Het is bovendien erg waarschijnlijk dat de betrokken burger deze schending van zijn privacy nooit te weten komt.

### 3.2 Het besturingssysteem

Helaas moeten we vaststellen dat de beveiliging van de meeste computers slecht is: vaak is er zelfs geen up-to-date antivirus programma noch een degelijke firewall aanwezig. Op de meeste computers draait een of andere variant van `Windows`, en vaak

[4]Een nieuwe versie van de software is beloofd voor de komende weken. Het is mogelijk dat in die versie reeds een aantal problemen opgelost zijn.

[5]Een afzonderlijk klavier om de PIN-code in te geven.

heeft de gebruiker administratieve rechten. Spyware, virussen en andere schadelijke programma's die de gebruiker ongewild binnenhaalt, kunnen dus onbeperkt wijzigingen aanbrengen aan de configuratie-bestanden en toepassingen installeren, wijzigen of weglaten; dus ook de privacy service en de eID software.

Het is erg riskant om een digitale handtekening te plaatsen op een dergelijke computer. Als deze handtekening al bewust door de gebruiker geplaatst is, dan nog bestaat de kans dat de gebruiker een ander bestand ondertekent dan hij/zij vermoedt. (Zie ook sectie 3.1.)

**Betwisting van digitale handtekening**

Alhoewel de met de eID kaart geplaatste handtekening dezelfde rechtsgeldigheid heeft als een handgeschreven handtekening, bestaat de kans dat heel wat mensen hun digitale handtekening voor de rechtbank zullen betwisten, door aan te voeren dat er spyware op de PC aanwezig was op het ogenblik van het plaatsen van die handtekening. Elke beveiligingsexpert zal moeten toegeven dat dit met de huidige eID kaart een plausibel scenario is.

# 4 Actiepunten

- Het gebruik van de kaart door kinderen moet afgeraden worden. De gevaren waaraan ze zich blootstellen zijn vele malen groter dan wanneer ze de kaart niet gebruiken.
- Er moet een eID roadshow komen, maar niet om het gebruik van de kaart aan te moedigen, wel om de mensen te wijzen op een verantwoord gebruik van de kaart. Zo is het zeker af te raden de kaart te gebruiken op andere locaties (zeker indien men de PIN-code moet ingeven via het toetsenbord van de computer).
- Het gebruik van "primitieve kaartlezers" moet ontraden worden.
- Het ontwikkelen van nieuwe toepassingen moet door de overheid afgeremd worden tot de problemen volledig opgelost zijn. Het lijkt daarom niet aangewezen om met de eID kaart databanken die persoonlijke medische gegevens bevatten toegankelijk te maken.
- Bedrijven zouden slechts toepassingen voor de eID kaart mogen aanbieden na goedkeuring door de commissie ter bescherming van de persoonlijke levenssfeer. De commissie zal dan vooral moeten nagaan of "identificatie m.b.v. van de eID kaart" echt noodzakelijk is voor die toepassing.
- Het gebruik van de kaart als toegangsmiddel tot bijv. fitness-centra, moet aan strikte voorwaarden onderworpen worden. Bijv. de computer met kaartlezer mag niet verbonden zijn met het Internet; de software moet aan minimale veiligheidseisen voldoen, etc.
- De bestaande software moet dringend aangepast worden. Heel wat van de hierboven geschetste problemen kunnen echter **niet** opgelost worden door alleen de software aan te passen. Immers, een toepassing hoeft geen gebruik te maken van deze software. Nieuwe software versies moeten uitvoerig geëvalueerd en getest worden door experten.
- Het ontwerp van de kaart moet dringend herzien worden, zodat misbruiken zoveel mogelijk vermeden kunnen worden.